

Remarks

This application is a continuation of parent application Serial No. 08/933,541, filed September 9, 1997. In order to expedite the prosecution of this application, the newly presented claims and the following remarks address the rejections cited in the Office Action of the parent application dated September 3, 1999.

The Examiner in the parent application had rejected prior claims 1-10 under 35 U.S.C. §101 as being non-statutory. In addition, claims 1-5 and 7-10 were rejected under 35 U.S.C. §102(a) as being anticipated by Biham et al, "A New Cryptanalytic Attack on DES" and claims 2-5 and 7-8 were rejected under 35 U.S.C. §103 as being unpatentable over admitted prior art in view of Force et al, U.S. Patent 5,533,123 (hereinafter Force) and Kahn, "Seizing the Enigma," as referred to in Reference R in view of Force. In response thereto applicants have cancelled claims 1 through 10.

The Examiner also rejected claims 27-39 under 35 U.S.C. §101 because they are not in one or the statutory classes and under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. In addition, claims 35-39 were rejected under 35 U.S.C. §112, first paragraph, because the specification does not reasonably provide enablement for these claims and under 35 U.S.C. §102(b) as being anticipated by Carswell et al, U.S. Patent 5,365,591 and Force. In response thereto applicants have cancelled claims 27-39.

The Examiner rejected claims 11-26 under 35 U.S.C. §101 as being non-statutory. In response thereto, applicants have cancelled prior claims 11-26 and incorporated their subject matter into newly presented claims 40 and 43-53. Applicants note that prior claims 11-26 were not rejected on prior art. In addition, applicants have incorporated the subject matter of prior claims 3, 4 and 6 into newly presented claims 40, 42, and 41, respectively.

Newly presented claims 40-53 reflect the use of a second cryptography device receiving electrical signals from and transmitting electrical signals to a first cryptography device to determine secret information stored only in the first cryptographic device and to generate an output stream containing secret information, thereby relieving any abstraction. Four embodiments for determining the secret information within the second cryptography are reflected in the newly presented claims.

The first embodiment, recited in claims 40-42, uses a method based on RSA implementations utilizing the Chinese Remainder Theorem and implementations using the Rabin Signature Scheme. The second embodiment, recited in claims 43-47, uses a method based on Fiat-Shamir Authentication Scheme. The third embodiment, recited in claims 49-50, comprises a method using register faults and RSA implementations not utilizing the Chinese Remainder Theorem. The final embodiment, recited in claims 51-53, comprises a method based on Schnorr's Authentication scheme.

Applicants submit that newly presented claims 40-53 obviate the Examiners §101 rejection that "there are not independent physical acts that can be construed as significant pre- or post-computer

process activity” based on Section IV.B.2(d)(ii)-(iii) of the “Examination Guidelines for Computer Related Inventions” [hereinafter Guidelines]. The Guidelines state that “if a claim requires acts to be performed to create data that will then be used in a process representing a practical application of one or more mathematical operations, those acts must be treated as further limiting the claim beyond the mathematical operation(s) per se.”

Newly presented independent claims 40 and 49 require the step of placing the first cryptography device under stress to create the incorrect signature to be transmitted and processed by the second cryptography device; thus, creating data to be used in the process. Newly presented independent claim 43 requires the step of generating an electrical signal containing a subset of integers S and transmitting this electrical signal to the first cryptography device. The subset of integers induces the first cryptography device to create a second authentication value, based on the subset of integers, to be processed by the second cryptography device; thus, creating data to be used in the process. Newly presented independent claim 51 requires the steps of transmitting a challenge and then transmitting the same challenge again from the second cryptography device to the first cryptography device. In response to these challenges, the first device creates two different responses which are then processed in the second device; thus, creating data to be used in the process.

In addition, the Examiner states that the claimed steps are abstract manipulation without any limitation to a practical application, citing Section IV.B.2(e) of the Guidelines. Applicants respectfully submit that the newly presented claims obviate this rejection because they recite generating an output electrical signal containing secret information stored in the first cryptography device. This output can then be compared against known values to determine the security of the first cryptography device. This invention has many practical applications particularly in the areas of electronic commerce and electronic communications which depend on difficult-to-crack cryptosystems to prevent unauthorized access to secured information. This invention allows designers of these systems to determine whether the cryptosystem or cryptography device being used in their implementation is vulnerable to an external attack.

In addition, the Examiner states that prior claims 1-26 comprise a series of steps to be performed on a general, non-specific, computer citing Section IV.B.2(a)(i) and (ii). Applicants note that this section of the Guidelines relates specifically to product claims. Because newly presented claims 40-54 are process claims, applicants submit that this rejection is obviated.

The subject matter of prior claim 3 of placing the first cryptography device under physical stress has been incorporated into newly presented independent claim 40. Newly presented claim 42 is a dependent claim which incorporate the subject matter of prior claims 4 wherein the physical stress includes atypical voltage levels, higher speed, or radiation. Applicants submit that newly presented claim 42 is patentable both for its own recited limitations and in view of the parent claim. In addition, the cited references do not teach or suggest placing a first cryptography device under physical stress

combined with a method to determine secret information in a second cryptography device using a processor based on RSA implementations utilizing the Chinese Remainder Theorem and implementations using the Rabin Signature Scheme.

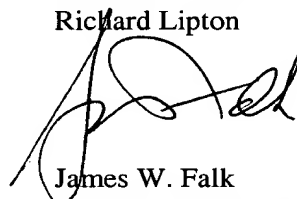
Similarly, newly presented claim 41 is a dependent claim which incorporates the subject matter of prior claim 6. Newly presented claim 41 recites a method of generating "a digital signature which may be separated into linear components." Applicants agree that taken individually the separation of a digital signature into linear components is known in the art. However, applicants submit that the cited references do not teach or suggest the novel use of implementations having linear components with the method to determine secret information contained in a first cryptography device using a second cryptography device based on RSA implementation utilizing the Chinese Remainder Theorem and implementations using the Rabin Signature Scheme.

Accordingly applicants submit that newly presented claims 40-53 are clearly allowable. Entrance of this Amendment and favorable consideration and allowance of claims 40-53 are therefore respectfully requested.

Applicants believe that this application is now in condition to be passed to issue, and such action is also requested. However, if the Examiner believes it would in any way facilitate the prosecution of this application, the Examiner is invited to telephone applicants' attorney at the number given below.

Respectfully submitted,

Dan Boneh
Richard A. DeMillo
Richard Lipton



James W. Falk
Attorney of Record
Reg. No. 16154
(973) 829-2360

Telcordia Technologies, Inc.
445 South Street
Morristown, NJ 07960

Date: April 25, 2000